A Hierarchical Security Architecture for Cyber-Physical Systems

Quanyan Zhu[1], Craig Rieger[2] and Tamer Başar[1]

[1] Coordinated Science Laboratory
Department of Electrical and Computer Engineering

University of Illinois at Urbana-Champaign

[2] Idaho National Laboratory

4th International Symposium on Resilient Control Systems

Boise, ID, 2011

Outline

- Security issues in cyber-physical systems
  - Introduction and motivation
- Hierarchical security architecture
  - Problem identification
  - Illustration through examples
- Challenges and future work

Security Issues in Cyber-Physical Systems

- Integration of IT infrastructure with industrial control systems has exposed a closed network of systems to the publicly accessible network:
  - Cost and performance benefits,
  - Vulnerable to security risks and threats.

- Conventional IT solutions to security can not be directly applied.
  - Security objectives
  - Security architecture
  - Quality-of-service requirement

- Reliability and robustness in a relatively isolated control system vs. resilience and security in an integrated and open system.

THE WALL STREET JOURNAL.
WSJ.com

TECHNOLOGY | APRIL 8, 2009

Electricity Grid in U.S. Penetrated By Spies

By SIOBHAN GORMAN

Associated Press

Robert Moran monitors an electric grid in Dallas. Such infrastructure grids across the country are vulnerable to cyberattacks.

WASHINGTON -- Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials.

The spies came from China, Russia and other countries, these officials said, and were believed to be on a mission to navigate the U.S. electrical system and its controls. The intruders haven't sought to damage the power grid or other key infrastructure, but officials warned they could try during a crisis or war.

The Washington Post

Cyber Incident Blamed for Nuclear Power Plant Shutdown

By Brian Krebs
washingtonpost.com Staff Writer
Thursday, June 5, 2008; 1:46 PM

PMA nuclear power plant in Georgia was recently forced into an emergency shutdown for 48 hours after a software update was installed on a single computer.

The incident occurred on March 7 at Unit 2 of the Hatch nuclear power plant near Baxley, Georgia. The trouble started after an engineer from Southern Company, which manages the technology operations for the plant, installed a software update on a computer operating on the plant's business network.

COMPUTERWORLD

Siemens: Stuxnet worm hit industrial systems

Robert McMillan

September 14, 2010

A sophisticated worm designed to steal industrial secrets and disrupt operations has infected at least 14 plants, according to Siemens.
Called Stuxnet, the worm was discovered in July when researchers at VirusBlokAda found it on computers in Iran. It is one of the most sophisticated and unusual pieces of malicious software ever created -- the worm leveraged a previously unknown Windows vulnerability (now patched) that allowed it to spread from computer to computer, typically via USB sticks.

FAA official out amid sleeping-on-the-job cases

By **the CNN Wire Staff**
April 14, 2011 11:04 a.m. EDT

The Federal Aviation Administration has disclosed controllers have fallen asleep in at least six instances this year.

STORY HIGHLIGHTS

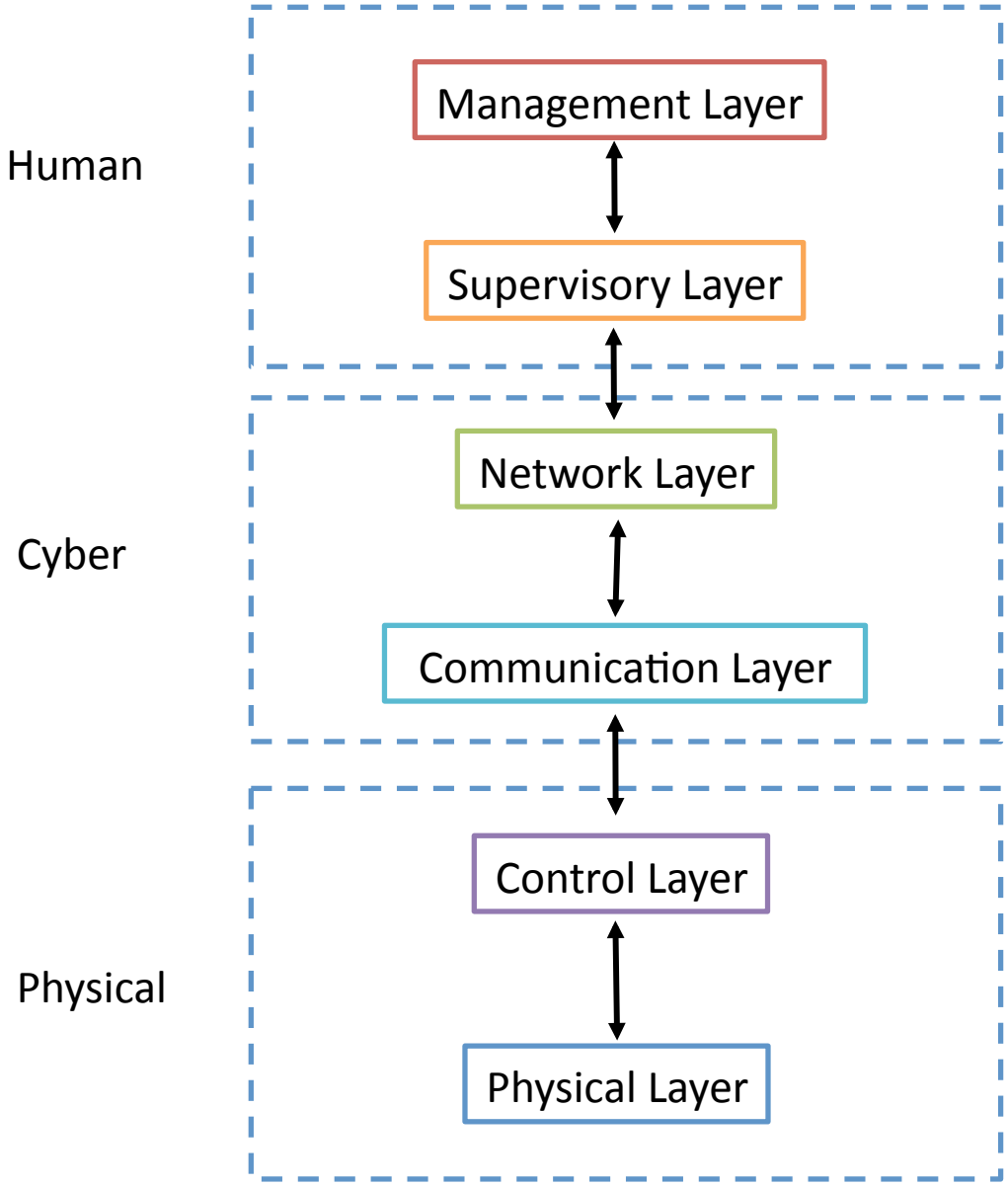
- The FAA is looking for a new chief of air traffic control
- The agency is trying to correct "unprofessional conduct"
- The FAA is placing an extra overnight shift controller at

Washington (CNN) -- The Federal Aviation Administration official in charge of operating the air traffic control system has resigned amid revelations that several controllers have fallen asleep on the job this year, the FAA chief said Thursday

Stepping down is Hank Krakowski, who has been the head of the FAA Air Traffic Organization. David Grizzle, the FAA's chief counsel, will be the acting chief of the unit during a search to fill the post, according to Randy Babbitt, the agency's administrator.

"Over the last few weeks we have seen examples of unprofessional conduct on the part of a few individuals that have rightly caused the traveling public to question our ability to ensure their safety. This conduct must stop immediately," Babbitt said in a statement.

Layered Architecture and Modularized Design



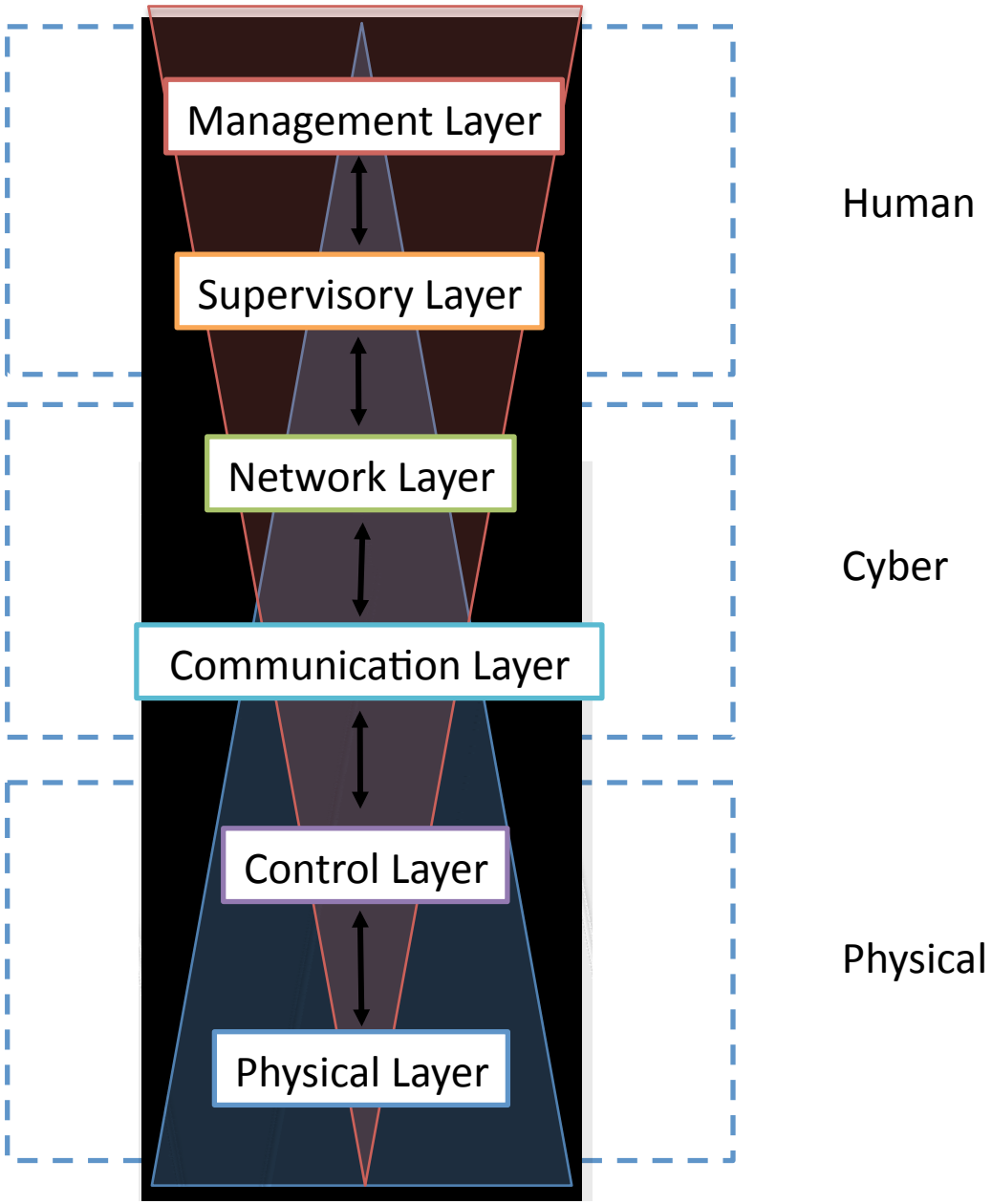
Flow control, PoA and PoI, data fusion, patching problem, pricing, demand response, market mechanism, etc.

IDS/IPS configuration and defense mechanism, CODIPAS learning algorithms, jamming, eavesdropping, data injection, secure distributed routing, reliability, stealthy attack, etc

H-infinity robust control, adaptive control, fault-tolerant control

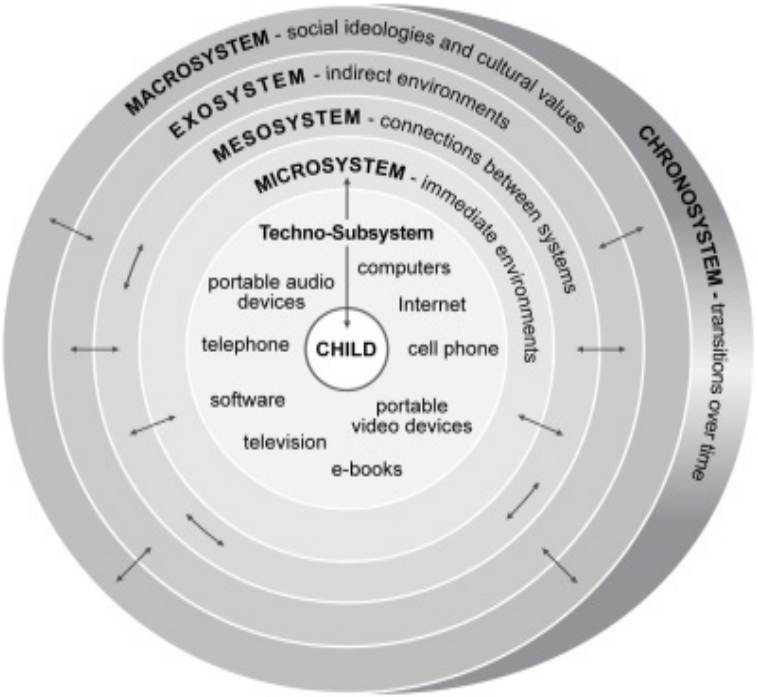
Red: Ongoing Work
Black: Future Work

Cross-Layer Design



Examples of Hierarchical Structures

Internet OSI Layering



Bronfenbrenner's Ecological Framework

Seven Dynamically Interacting Grids

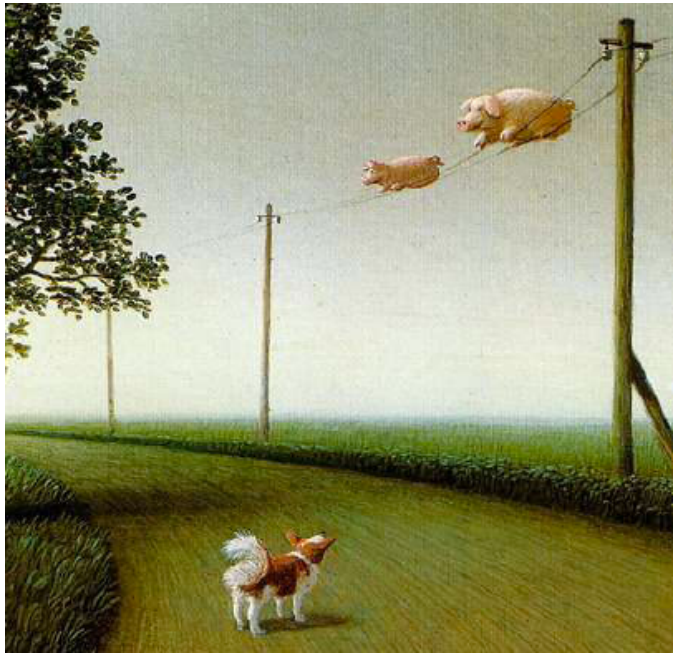
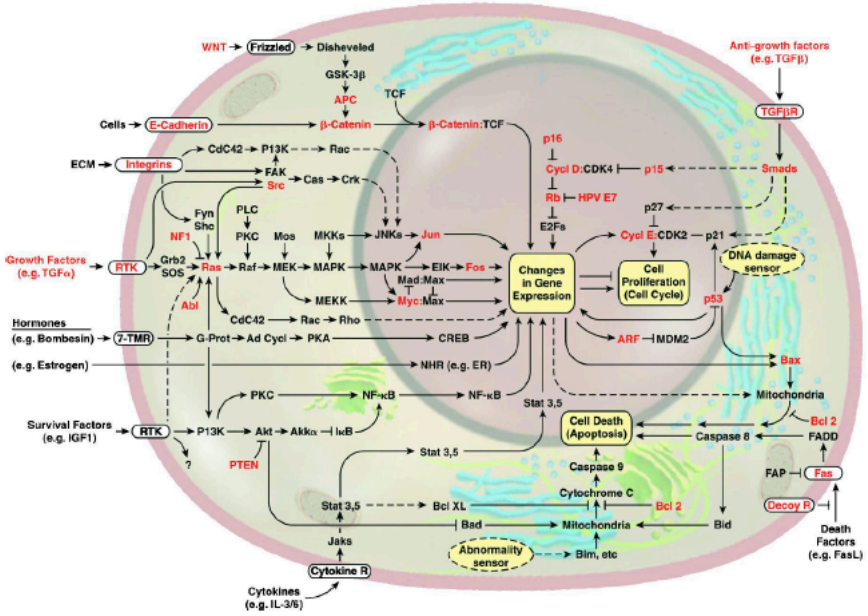


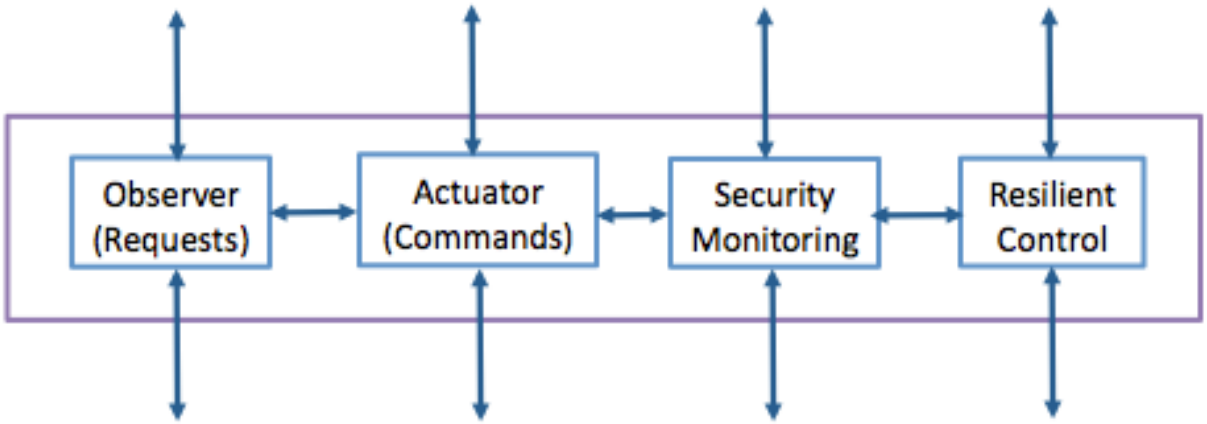
Illustration: Michael Sowa



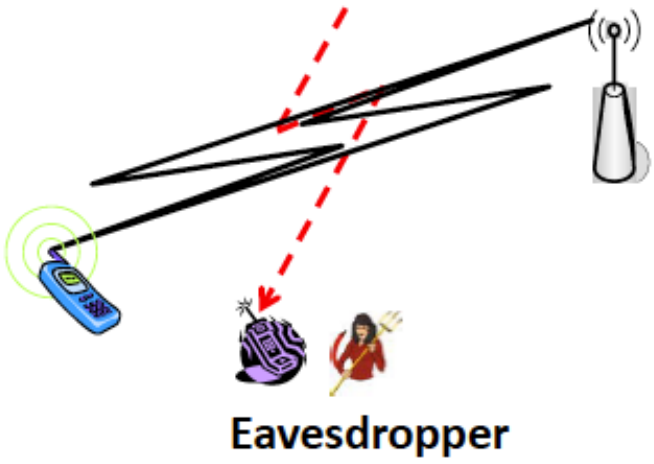
Hanahan and Weinberg, Cell, 2000

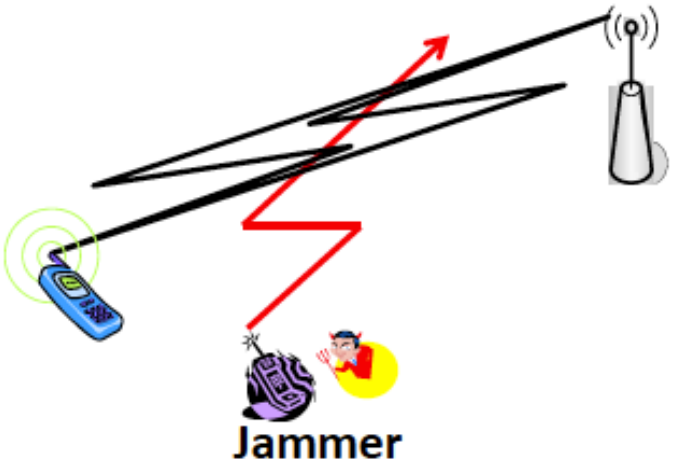
- Physical Layer
  - Protection against vandalism, environmental change, expected events.
  - Reliability
  - Maintenance
  - Modeling of complex systems

Control Layer

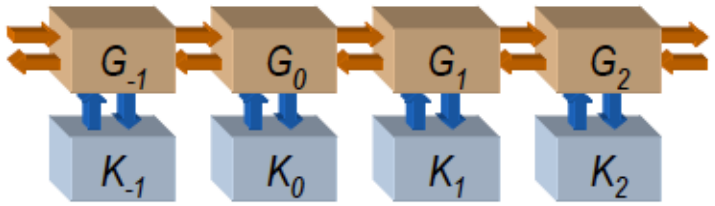


- Observer: reliable sensing and estimation
- Actuator: secure information flow
- Security monitoring: intrusion detection, prevention and response.
- Resilient control: methodology to ensure resilience, including diagnosis, fault-tolerance, adaptive control, reconfiguration, etc.



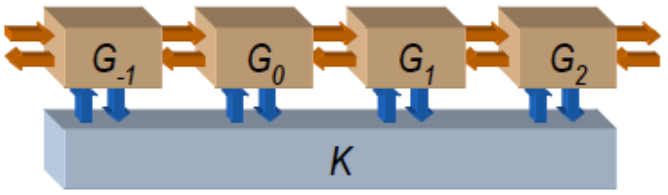


- Data communication layer: jamming and eavesdropping, etc.
- Network layer: secure routing, network formation and deployment, etc.



Decentralized Control

vs.



Centralized Control

$$\text{Price of Anarchy (PoA)} = \frac{\text{System Performance using Decentralized Control}}{\text{System Performance using Centralized Control}}$$

$$\text{Price of Information (PoI)} = \frac{\text{System Performance under OL information structure}}{\text{System Performance under FB information structure}}$$

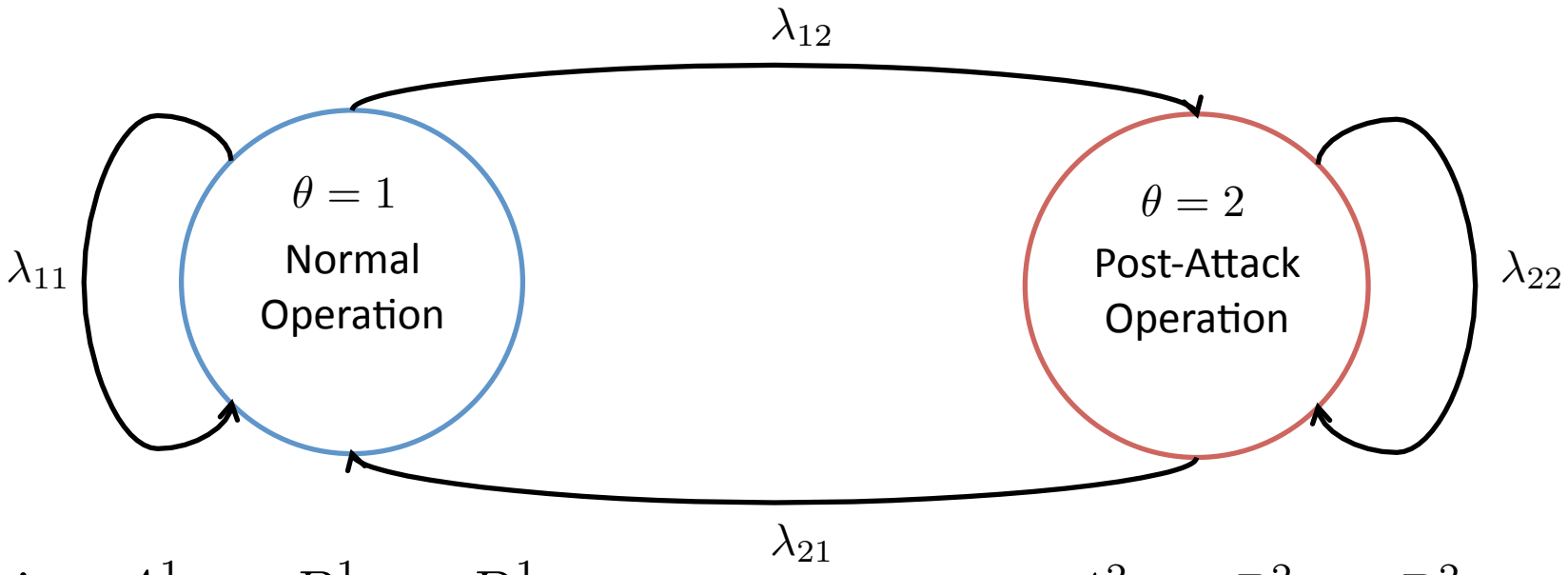
- Supervisory level: centralized vs. decentralized decision making, tradeoff between robustness and resilience.

- Management level: security policy, patch management, security investment decisions, vulnerability disclosure, etc.

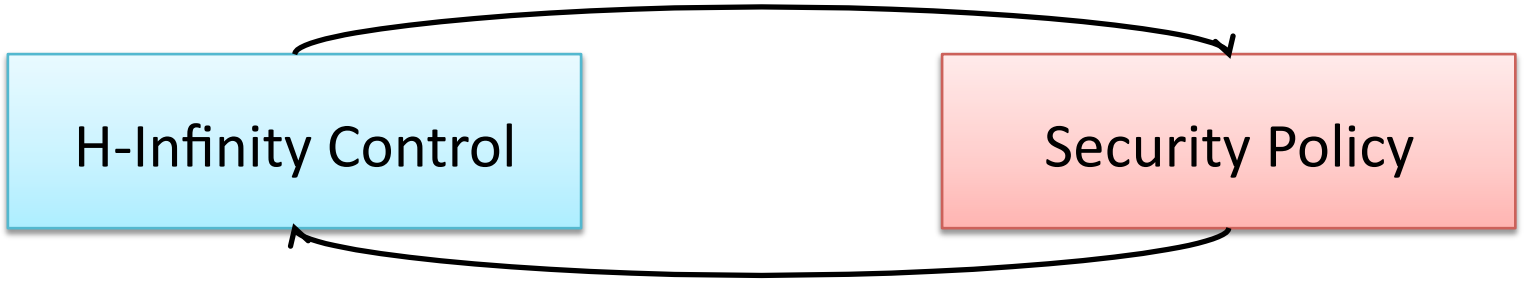
Illustration by Examples

1. Robust and Resilient Control
2. IDS/IPS Modeling in Control Systems
3. Secure Routing in the Smart Grid
4. Vulnerability Discovery and Disclosure
5. Pricing in Power Market

Resilient and Robust Control Design

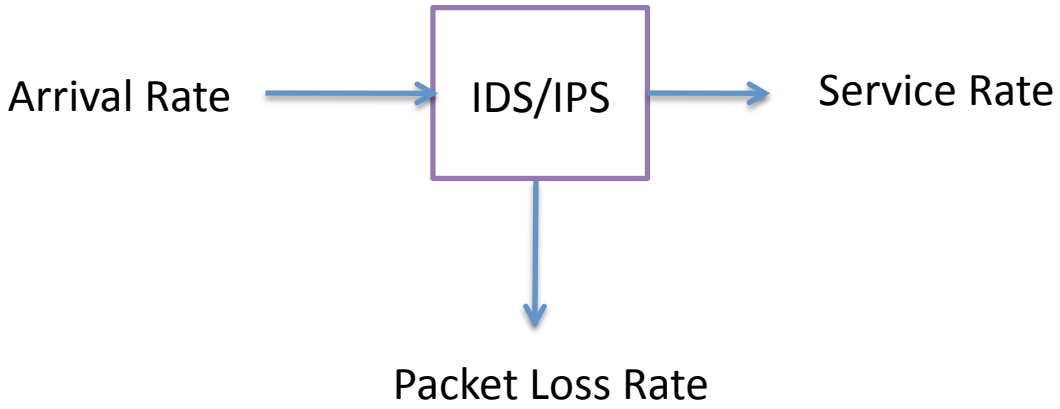


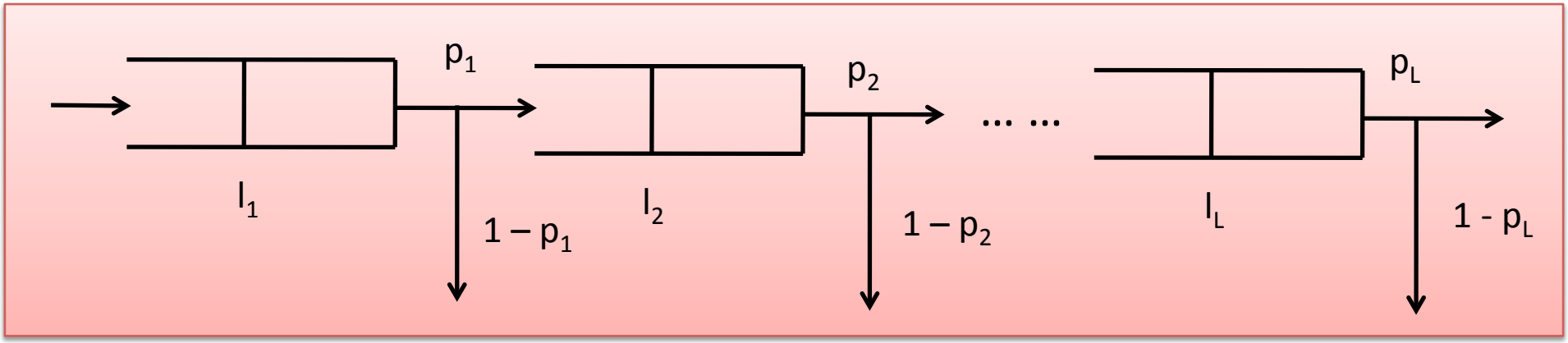
$$\dot{x} = A^1 x + B^1 u + D^1 w \qquad \dot{x} = A^2 x + B^2 u + D^2 w$$



Zhu and Başar, CDC 2011

Intrusion Detection/Prevention Systems

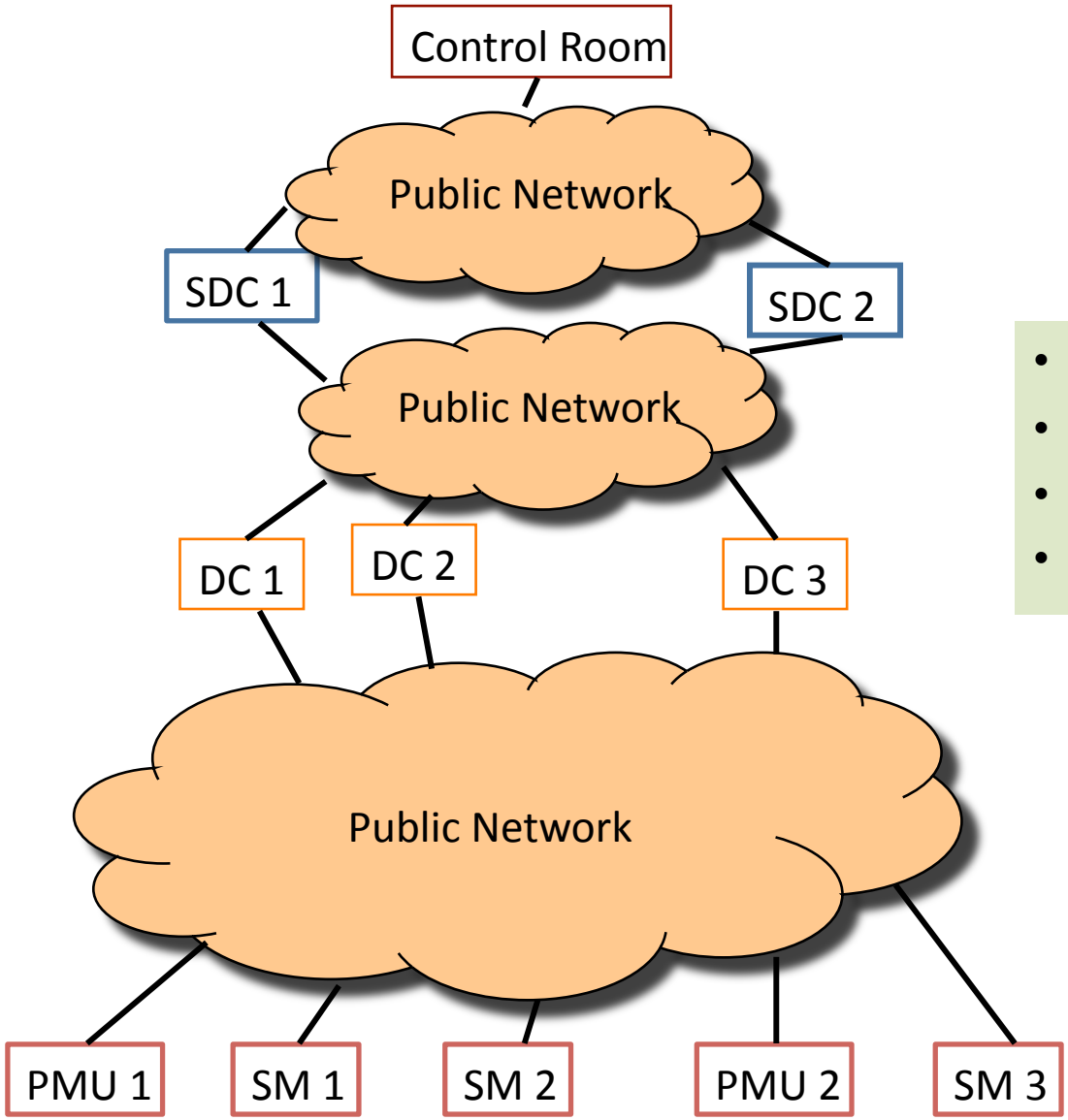




- 1 - p_i : packet drop rate
- μ_i : service rate
- M/M/1 queue

Zhu and Başar, CPS Week 2011

Communication/Network Layer: Secure Routing Problem

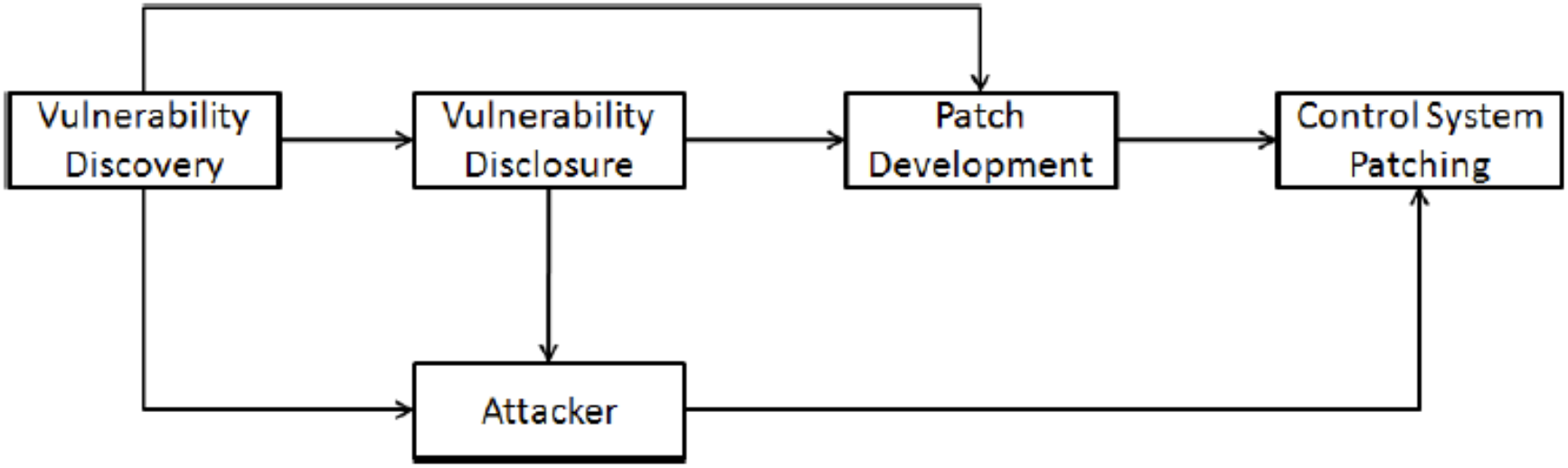


- Games-in-Games Structure
- Distributed Learning in Games
- Robustness vs. Resilience
- PoA and PoI

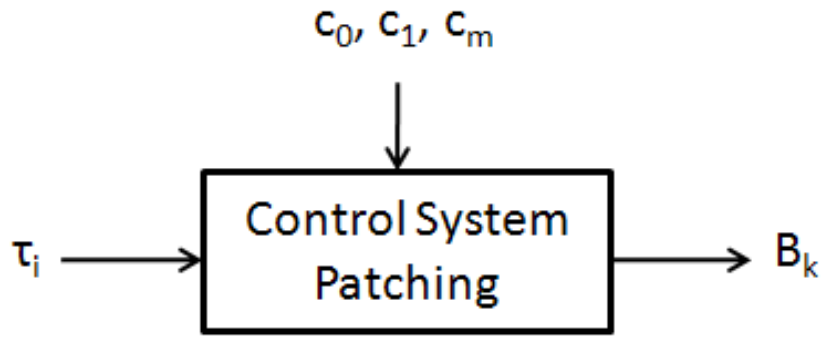
PMU: Phase Measurement Unit
SM: Smart Meter
SDC: Super Data Concentrator
DC: Data Concentrator

Zhu and Başar, CPS Week 2011

Management Layer: Software Vulnerability in Control Systems



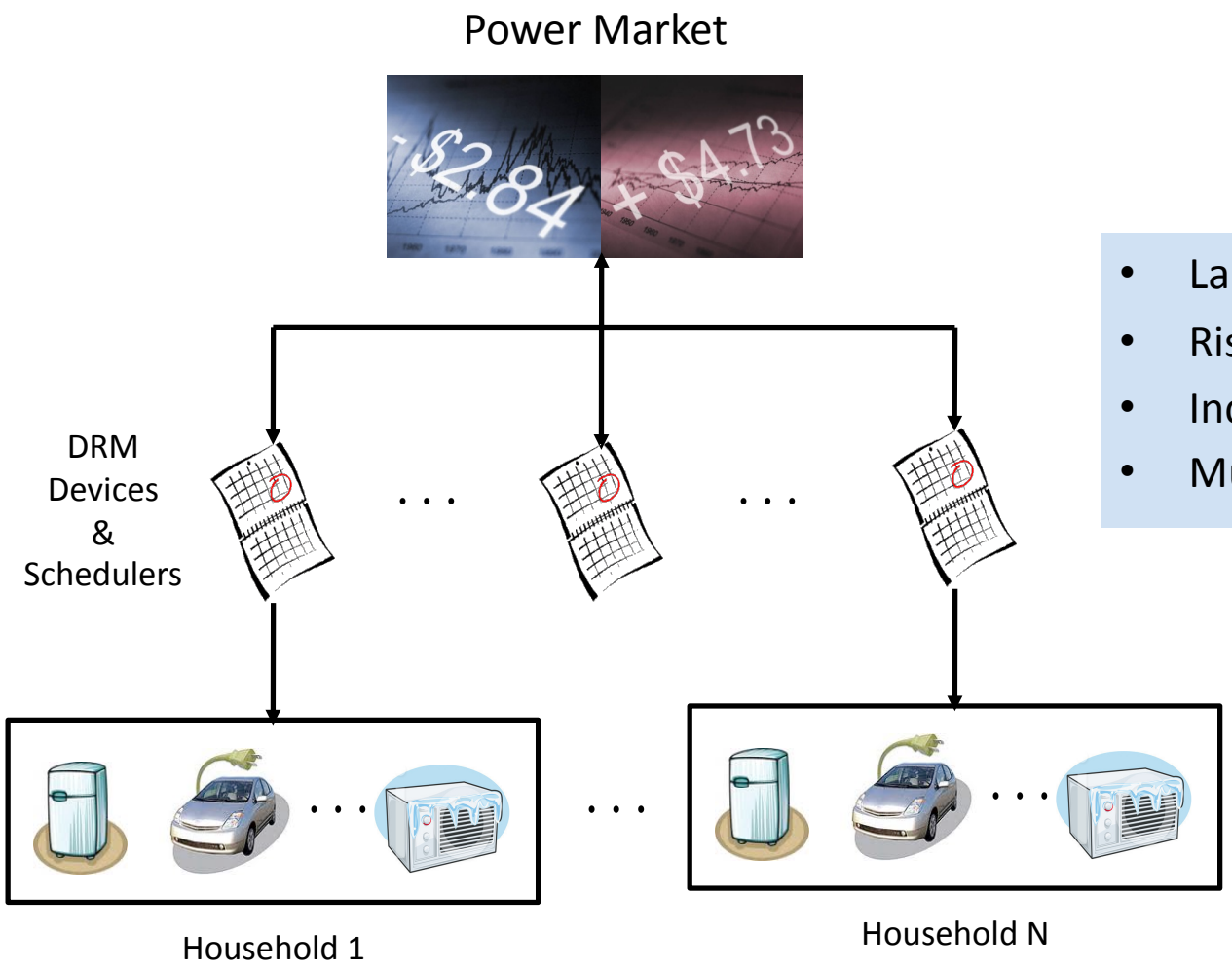
Flow Diagram of Software Vulnerability



Input-Output System Model

Quanyan Zhu et al. , CPSWeek 2011 Workshop.

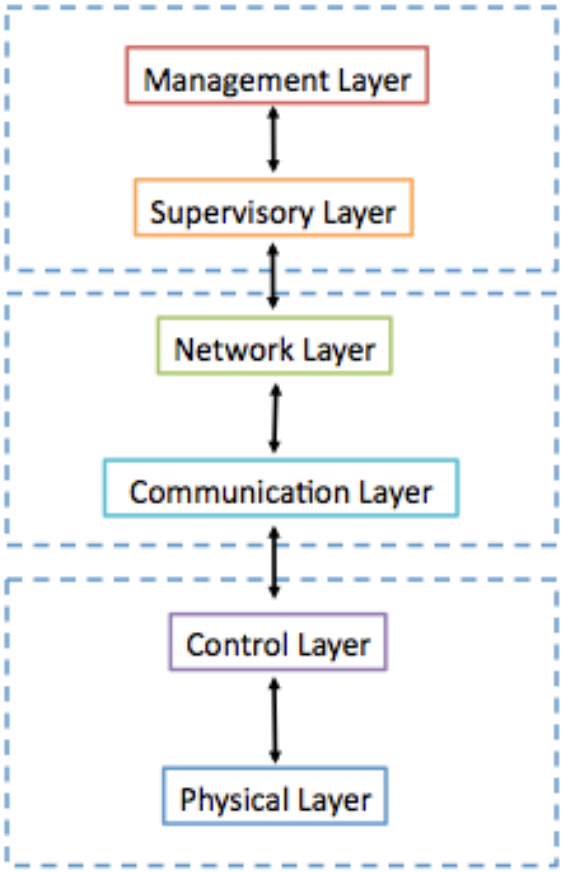
Management Layer: Dynamic Pricing Problems in SG



- Large population games
- Risk-sensitivity
- Incomplete information
- Multi-resolution framework

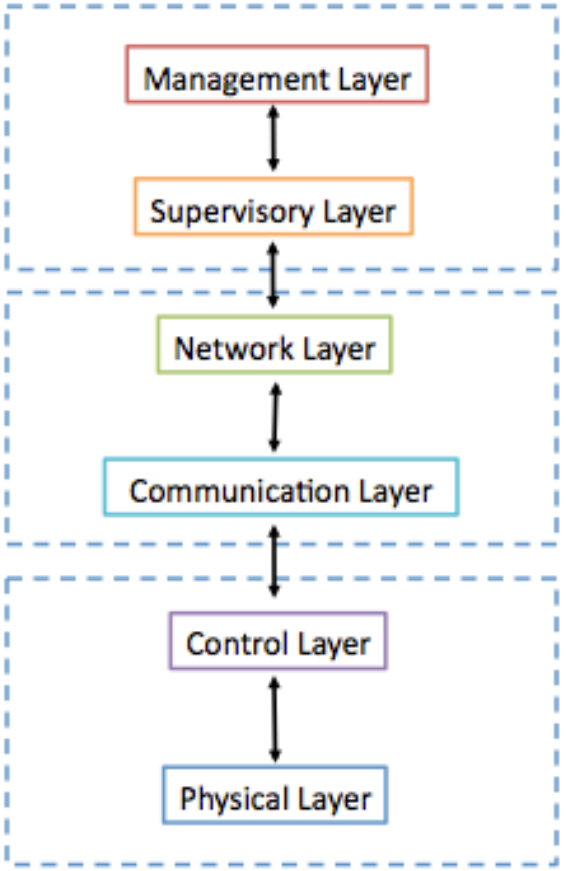
Conclusion (1)

- Modular and Cross-Layer Design
  - Physical/Control layer: H-infinity robust control, adaptive control, fault-tolerant control, etc.
  - Communications layer: IDS/IPS configuration and defense mechanism, CODIPAS learning algorithms, jamming, eavesdropping, data injection, etc.
  - Network layer: secure distributed routing, reliability, stealthy attack, etc.
  - Supervisory layer: flow control, PoA and PoI, data fusion, etc.
  - Management layer: patching problem, pricing, etc.



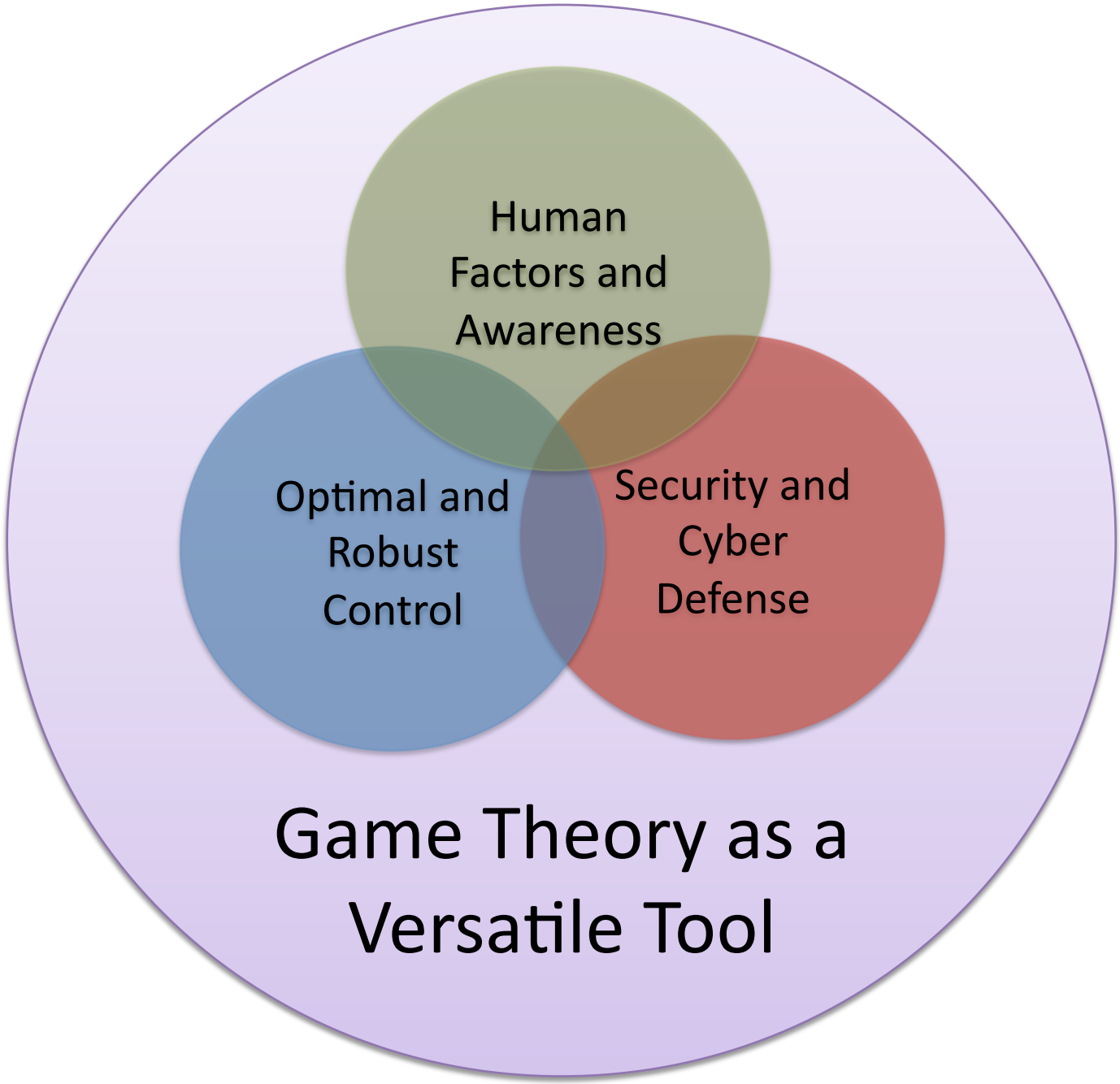
Conclusion (2)

- Layered control architecture facilitates the security problem identification at each layer of cyber-physical systems and modular analysis and design for the complex systems.
- Game theory is a useful tool to quantify robustness and resilience.
- Game theory enables cross-layer design and analysis for security issues in cyber-physical systems.



Future Directions:

- The tools can be generalized to study a broader class of problems in transportation systems.
- Towards online learning or computation at each layer.
- The framework can be applied to study multi-agent systems.


Human
Factors and
Awareness
Optimal and
Robust
Control
Security and
Cyber
Defense
Game Theory as a
Versatile Tool

Extended Hierarchical Architecture